

RHONDA JURGENS,  
Plaintiff,  
vs.  
BUILD.COM, INC.,  
Defendant.

This putative class action arises out of Defendant Build.com, Inc.’s alleged interception of its online customers’ names, addresses, telephone numbers, and credit card information (defined in the complaint, collectively, as “Credit Card Details”), and disclosure of those details to unrelated third parties, without the customers’ consent. The matter is now before the Court on Defendant’s motion (ECF No. 24) to dismiss the second amended complaint of named Plaintiff Rhonda Jurgens with prejudice, for failure to state a claim and lack of standing. For the following reasons, the Court will grant Defendant’s motion.

On or about March 29, 2014, Plaintiff used a computer to visit Defendant's website, on which consumers could purchase home improvement merchandise. On the website, Plaintiff selected kitchen plumbing hardware and added it to her online shopping cart, for a purchase price totaling \$703.53. When Plaintiff clicked a button to begin the check-out process, the website displayed a payment page, including a payment form

asking Plaintiff to enter her Credit Card Details. The payment page also included a button to “Review Order.”

According to the second amended complaint, the following then transpired:

16. Plaintiff entered her Credit Card Details on the Payment Page. As she did so, with each keystroke that appeared on her monitor display, her changes were transmitted to a file in her browser referred to as the “DOM” (Document Object Model)—an internal browser capture of the real-time state of an active web page—in this case, the Payment Page, the payment form on it, and the payment data Plaintiff entered on it.

17. The DOM is a transient storage file, incidental to the receipt and sending of web communications.

#### **B. Defendant’s Interception of Plaintiff’s Credit Card Details**

18. While Plaintiff entered her Credit Card Details on Defendant’s Page, as described above, it was not her intent to communicate with Defendant or any other party; rather, it was her intent to fill in the payment data in the payment form requested by Defendant, for transmittal to Defendant if and when she chose to click the button to confirm her purchase intent.

19. Plaintiff’s entry of Credit Card Details was an electronic communication to temporary browser storage, as described above, but not to Defendant, and Defendant did not have consent or the right in any way to intercept her Credit Card Details . . . .

ECF No. 22 ¶¶ 16-19.

Plaintiff alleges that Defendant intercepted her Credit Card Details “through the use of electronic devices known as JavaScripts (computer commands) transmitted to Plaintiff’s computer via the Internet from Defendant’s computer facilities.” *Id.* ¶ 21. These JavaScripts “were downloaded and executed on her computer because of Defendant’s explicit instructions, built into its Payment Page,” and Defendant intercepted

Plaintiff's Credit Card Details while those details "were temporarily stored in Plaintiff's browser, before transmission over the Internet." *Id.* ¶¶ 29, 39.

Plaintiff further alleges that "by operation of those same scripts," Defendant disclosed Plaintiff's credit card information to six or more third parties. *Id.* ¶¶ 24, 26. These third parties were "providers of services such as image and video advertising, user tracking and profiling, and tracking of user mouse movements and clicks—none of which is necessary to process payments." *Id.* ¶ 22. Plaintiff alleges that, for "other third parties, Defendant coded its Payment Page to restrict scripts . . . [such that] Defendant did not use the scripts to access Plaintiff's Credit Card Details in the DOM or disclose them to the third party." *Id.* ¶ 25. Plaintiff points to this "differential treatment" as evidence that "Defendant engaged in interception and disclosure of Credit Card Details in the DOM with knowledge and intent." *Id.*

According to Plaintiff, unrestricted JavaScripts are prone to privacy and security breaches, and because of these risks, such scripts are in violation of payment card industry standards and are not used by more security-conscious online retailers. In support of these allegations, Plaintiff cites news articles dated in 2011 and 2014. *Id.* ¶ 33 n.5. Plaintiff also states that the source of her information in this regard is her "counsel's investigation." *Id.* ¶ 34.

Although Plaintiff accessed Defendant's website and made her purchases on March 29, 2014, she did not file suit until December 30, 2016.<sup>1</sup> Plaintiff alleges that she

---

<sup>1</sup> Plaintiff's original complaint, filed in state court, alleged that Defendant's use of unrestricted JavaScripts to collect customers' credit card information violated Missouri

“did not have the technical knowledge or reasonable means to detect the [unrestricted JavaScripts] that Defendant executed on her computer” and to “understand[] their implications for privacy [and] security,” and that she only learned of this violation “through the investigation of her counsel in August 2016.” *Id.* ¶¶ 47, 48.

Plaintiff’s second amended complaint asserts three claims: (1) Violations of the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 (“ECPA”) 18 U.S.C. § 2511(1)(a) (Interception); (2) Violations of the Wiretap Act, 18 U.S.C. § 2511(1)(c) (Disclosure); and (3) Common-Law Unjust Enrichment. Plaintiff seeks injunctive relief, the maximum allowable statutory damages, punitive damages, and attorneys’ fees.

Plaintiff brings this action on her own on behalf and on behalf of two proposed classes: (1) a “Wiretap Act Class” encompassing “[a]ll individuals in the United States who used payment cards to purchase merchandise on the *www.build.com* website during the Wiretap Act Class Period,” defined as “two years preceding the date of filing of the Original Petition in this matter and extending to the date [of class certification]”; and (2) a “Missouri Class” encompassing “[a]ll individual Missouri citizens aged 18 years and over who used payment cards to purchase merchandise on the *www.build.com* website during the Missouri Class Period . . . where such merchandise was primarily for personal,

---

computer tampering and consumer protection statutes, and constituted an invasion of privacy and unjust enrichment under Missouri common law. Defendant removed the case to this Court on February 22, 2017, under the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d)(2). On July 10, 2017, with the Court’s leave, Plaintiff filed the second amended complaint now under consideration. For purposes of this motion only, Defendant does not contest that the second amended complaint “relates back” to Plaintiff’s original complaint under Federal Rule of Civil Procedure 15(c).

family, or household uses,” with the Missouri Class Period defined as “five years preceding the date of filing of the Original Petition in this matter and extending to the date of [class certification].” *Id.* ¶¶ 58-59.

### **ARGUMENTS OF THE PARTIES**

Defendant argues that Plaintiff fails to state a claim for violation of the Wiretap Act (Counts 1 and 2) because Plaintiff has not alleged any interception of an electronic communication. Defendant argues that, accepting Plaintiff’s allegations as true, Plaintiff’s Credit Card Details were acquired by Defendant from storage in Plaintiff’s computer, rather than, as required by the Wiretap Act, as part of an electronic communication that Plaintiff was transmitting beyond her own computer.

Alternatively, Defendant argues that to the extent Plaintiff implies that the communication of her Credit Card Details was not complete when it reached the storage in her computer, Plaintiff still fails to state a claim because the intended recipient of the communication was Defendant. Defendant notes that there is no private cause of action under the Wiretap Act against a person who is a party to the communication.

Defendant further argues that Plaintiff’s Wiretap Act claim is untimely under the Wiretap Act’s two-year statute of limitations, which runs from the date on which the plaintiff had a reasonable opportunity to discover the alleged violation. Defendant contends that Plaintiff had a reasonable opportunity to discover the alleged violation when she accessed Defendant’s payment page to purchase merchandise more than two years before filing suit.

With respect to the unjust enrichment claim (Count 3), Defendant argues that Plaintiff has failed to plead an injury-in-fact to give her standing. Defendant also contends that Plaintiff fails to state a claim because she has not identified a benefit she conferred on Defendant that would be unjust for Defendant to retain.

In response, Plaintiff argues that she has sufficiently alleged that Defendant intercepted her electronic communications at a time prior to the time Defendant became a party to those communications, which is enough to state a claim under the Wiretap Act. Specifically, Plaintiff points to her allegations that Defendant, using the unrestricted JavaScripts and without Plaintiff's consent, "recorded [Plaintiff's] keystrokes in a transient browser storage area used for receiving and sending web communications from the currently active web page." ECF No. 30 at 3. Plaintiff argues that the interception was contemporaneous with the transmission of the communications, that the communications were being made using a system affecting interstate commerce (the Internet), and that Defendant was not a party to the communications at the moment of interception because Plaintiff had not yet designated Defendant to process her payment. Plaintiff contends that "[t]here is also nothing in the statute that requires Plaintiff to identify the other parties, if any, to her communications." *Id.* at 11.

Plaintiff also argues that her Wiretap Act claims are not time-barred because she filed suit less than two years from the time she had a reasonable opportunity to discover the violation. Plaintiff contends, as she did in her complaint, that she first learned of Defendant's conduct through her attorney's investigation in August 2016, and that she lacked the technical knowledge or skill to discover the violation on her own.

With respect to her unjust enrichment claim, Plaintiff argues that she has sufficiently pled an injury in fact for purposes of standing, as well as facts in support of each element of an unjust enrichment claim, by alleging that part of the \$703.53 she paid for the merchandise (which merchandise Plaintiff acknowledges she received in full) should have been, but was not, spent on adequate data security measures.

In reply, Defendant reiterates that the allegations in the complaint conclusively demonstrate that no Wiretap Act violation occurred, that the Wiretap Act claims are untimely in any event, and that Plaintiff lacks standing and fails to adequately allege a claim for unjust enrichment.

### **DISCUSSION**

Pursuant to Federal Rule of Civil Procedure 12(b)(6), “a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Wartman v. United Food & Commercial Workers Local 653*, 871 F.3d 638, 640 (8th Cir. 2017) (citation omitted). Moreover, “Article III standing is a threshold question in every federal court case,” and “requires three elements: (1) injury in fact; (2) a causal connection between the injury and the conduct complained of; and (3) the likelihood that the injury will be redressed by a favorable decision.” *E.L. by White v. Voluntary Interdistrict Choice Corp.*, 864 F.3d 932, 935 (8th Cir. 2017) (citations omitted).

On a motion to dismiss for failure to state a claim or for lack of standing, the reviewing court accepts the plaintiff’s factual allegations as true and draws all reasonable inferences in favor of the nonmoving party. *Torti v. Hoag*, 868 F.3d 666, 671 (8th Cir. 2017) (failure to state a claim); *E.L. by White*, 864 F.3d at 935 (standing). But “[c]ourts

are not bound to accept as true a legal conclusion couched as a factual allegation, and factual allegations must be enough to raise a right to relief above the speculative level.” *Torti*, 868 F.3d at 671 (citations omitted).

### **Wiretap Act (Counts I and II)**

“The post-ECPA Wiretap Act provides a private right of action against one who ‘intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.’” *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (citing 18 U.S.C. § 2511(1)(a); 18 U.S.C. § 2520 (providing a private right of action)). The Act also imposes liability on a person who “intentionally discloses” the contents of an electronic communication, “knowing or having reason to know” the communication was intercepted in violation of the Wiretap Act. 18 U.S.C. § 2511(1)(c). “Thus, interception is a necessary element for each type of violation.” *Bruce v. McDonald*, No. 3:13CV221-MHT, 2014 WL 931522, at \*2 (M.D. Ala. Mar. 10, 2014).

“A plaintiff pleads a prima facie case [of interception] under the Act by showing that the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.” *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 135 (3d Cir. 2015) (“Google”).

The Wiretap Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). An “electronic communication” is



“any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” *Id.* § 2510(12).

“The Act does not explicitly require that the acquisition of a communication occur contemporaneously with the transmission of the communication. Nonetheless, courts interpreting this language have uniformly concluded that an intercept requires contemporaneity.” *Luis v. Zang*, 833 F.3d 619, 627 (6th Cir. 2016) (collecting cases); *see also Porters Bldg. Ctrs., Inc. v. Sprint Lumber*, No. 16-06055-CV-SJ-ODS, 2017 WL 4413288, at \*8-9 (W.D. Mo. Oct. 2, 2017) (“The Eighth Circuit has not decided this particular issue, but most courts have determined interception must occur during transmission. The Court agrees with the findings of the majority of the courts.”) (internal citations omitted). These courts have reasoned that contemporaneity is necessary to distinguish “electronic communications” (the subject of the Wiretap Act, as amended by Title I of the ECPA) from “electronic storage” (the subject of Title II of the ECPA, also known as the “Stored Communications Act,” which covers access to electronic information stored in third party computers).<sup>2</sup> *See, e.g., Luis*, 833 F.3d at 627-28 (“Once the transmission of the communication has ended, the communication ceases to be a communication at all. The former communication instead becomes part of ‘electronic storage.’”).

Liability under the Wiretap Act is also subject to certain statutory exceptions, including, as relevant here, an exception for parties to the communication:

---

<sup>2</sup> Plaintiff does not assert a claim under the Stored Communications Act.

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication . . . .

18 U.S.C. § 2511(2)(d) (“party exception”).

Finally, “[a] civil action under [the Wiretap Act] may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.” 18 U.S.C. § 2520(e).

**a. Party Exception**

Taking Plaintiff’s well-pled allegations as true, if there was an “electronic communication” here, Defendant was a party to it. Indeed, Plaintiff alleges that the entry of her Credit Card Details was “an electronic communication to temporary browser storage,” or the “DOM,” which Plaintiff describes as “a transient storage file, incidental to the receipt and sending of web communications,” for eventual “transmittal to Defendant.”<sup>3</sup> ECF No. 22 ¶¶ 17-19. While “[t]ransmissions of completed online forms” on a website “constitute electronic communications,” *In re Pharmatrak, Inc.*, 329 F.3d at 18, the intended recipient of such transmission is a party to the communication, *Google*,

---

<sup>3</sup> Plaintiff perhaps uses the phrase “transient storage” to allude to a line of cases holding that communications—in particular, email messages—that are acquired by a third party while in “transient electronic storage” on the way to their final recipient, satisfy any “contemporaneity” requirement under the Wiretap Act. *E.g.*, *United States v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005) (holding that communications “en route to the intended recipients” constitute electronic communications even if the data is acquired by a third party while temporarily stored in a network computer along the route to the final destination); *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 705-06 (7th Cir. 2010), as amended (Nov. 29, 2010). But these cases do not save Plaintiff’s claim because, even if Plaintiff’s communications were acquired from transient storage and thus “contemporaneously” with transmission, they were acquired by the intended recipient of the communication, and such acquisition is not actionable under the Wiretap Act.

806 F.3d at 143 (3d Cir. 2015). As a party to the communication, Defendant is exempt from liability under the Wiretap Act.<sup>4</sup>

**b. Alternative Allegations**

To avoid the party exception, Plaintiff attempts to plead that the intended recipient of her “electronic communications” was the DOM on her own computer. In addition to contradicting the allegations discussed above, the Court agrees with Defendant that Plaintiff’s interactions with her own computer were not “communications” at all.<sup>5</sup> *See Google*, 806 F.3d at 143 (“Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient.”).

And if they were communications, then, according to Plaintiff’s own allegations, they were made within the confines of Plaintiff’s own computer “before transmission over the Internet.” ECF No. 22 ¶ 39. As such, they were not “electronic communications” transmitted by a system that affects interstate commerce, as required under the Wiretap Act. *See, e.g., United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011) (“[U]se of a keylogger will not violate the Wiretap Act if the signal or

---

<sup>4</sup> The party exception does not apply where the party intercepted a communication “for the purpose of committing any criminal or tortious act” in violation of federal or state law, 18 U.S.C. § 2511(2)(d), which is “*independent* of the intentional act of recording,” *Google*, 806 F.3d at 145 (citing *Caro v. Weintraub*, 618 F.3d 94, 100-101 (2d Cir. 2010)). But Plaintiff has neither alleged nor argued that Defendant intercepted or disclosed her communications for the purpose of committing a crime or a tort independent of the interception itself, and no such purpose is evident from the complaint.

<sup>5</sup> Plaintiff seems to acknowledge this, alleging at one point that “[w]hile Plaintiff entered her Credit Card Details on Defendant’s Page, as described above, it was not her intent to communicate with Defendant *or any other party*.” ECF No. 22 ¶ 18 (emphasis added).

information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed.”); *United States v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004) (holding that “[t]he acquisition of internal computer signals that constitute part of the process of preparing a message for transmission” are not “electronic communications” because they are “not transmitted by a system that affects interstate . . . commerce,” notwithstanding that the computer has a network connection to the Internet) (emphasis removed). Thus, Plaintiff’s Wiretap Act claims must be dismissed in any event.

**c. Statute of Limitations**

For the reasons set forth above, Plaintiff’s Wiretap Act claims fail on the merits. The Court also concludes that they are time-barred, as Plaintiff filed suit more than two years after the date upon which she first had a reasonable opportunity to discover the violation. *See* 18 U.S.C. § 2520(e). “[T]he ‘violation’ that is referenced in the statute is the interception of the communication, not the injury caused by the interception, [and] the [p]laintiff[] only need to be on inquiry notice of the violation to commence the statute of limitations period.” *In re Trilegiant Corp., Inc.*, 11 F. Supp. 3d 82, 111 (D. Conn. 2014).

The alleged violation here was Defendant’s use of unrestricted JavaScripts in the computer code for Defendant’s payment page, and Plaintiff had reasonable opportunity to discover this violation when she first accessed this payment page on March 29, 2014, more than two years before filing suit. Plaintiff cites articles dating back to 2011 for the proposition that unrestricted JavaScripts were known to contain security risks. And there is no allegation that Defendant concealed its use of unrestricted JavaScripts in its

computer code, or that the scripts were undiscoverable.<sup>6</sup> Indeed, Plaintiff alleges that her attorney was able to discover the scripts, and nothing in the complaint suggests the attorney (or anyone else) was prevented from discovering them sooner.

Although Plaintiff claims she did not have the technical knowledge to identify the computer code on her own, her lack of technical expertise is not a reason to toll the statute of limitations here. *See, e.g., Thompson v. Ret. Plan for Emps. of S.C. Johnson & Sons, Inc.*, 716 F. Supp. 2d 752, 772 (E.D. Wis. 2010) (rejecting the plaintiffs’ argument that they could not “discover” their ERISA injury from the highly technical plan documents, and reasoning that such an argument would “suggest[] that any plaintiff whose claim involves complicated and technical information may sidestep the statute of limitations until he understands that information”), *aff’d*, 651 F.3d 600 (7th Cir. 2011).

### **Unjust Enrichment (Count III)**

Putting aside the question of whether Plaintiff has standing to assert an unjust enrichment claim, the Court finds that she fails to state such a claim. Under Missouri law, “[u]njust enrichment requires a showing that: (1) the plaintiff conferred a benefit on the defendant; (2) the defendant appreciated the benefit; and (3) the defendant accepted and retained the benefit under inequitable and/or unjust circumstances.” *Hargis v. JLB Corp.*, 357 S.W.3d 574, 586 (Mo. 2011) (citations omitted). “The third element . . . is considered the most significant and the most difficult of the elements,” and “there can be

---

<sup>6</sup> Tellingly, as Defendant notes, Plaintiff defines the proposed “Wiretap Act Class” as individuals who purchased merchandise on Defendant’s website within “two years preceding the date of filing of the Original Petition,” which would exclude Plaintiff.

no unjust enrichment if the parties receive what they intended to obtain.” *Sparks v. PNC Bank*, 400 S.W.3d 454, 460 (Mo. Ct. App. 2013).

Plaintiff claims that the unjust enrichment here is the money she paid to Defendant for merchandise, which she received in full, because part of that money should have gone to pay for better data security measures. But Plaintiff does not allege any facts giving rise to a reasonable inference that any specific portion of the money she paid was intended or required to be spent on data protection. As such, Plaintiff has failed to state a claim that she conferred a benefit on Defendant the retention of which would be inequitable. *See Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016) (dismissing an unjust enrichment claim based on allegations that the plaintiff paid a subscriber fee to a website operator who subsequently disclosed personal information to third parties, where the plaintiff did not “allege that any specific portion of his subscriber fee went toward data protection or that [the defendant] agreed to provide additional protection to paid subscribers that it did not also provide to non-paid subscribers”); *In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) (dismissing an unjust enrichment claim which alleged that health insurance premiums should have gone toward better security measures on the grounds that the plaintiffs “d[id] not claim that they were denied [health insurance] coverage or services in any way whatsoever,” the plaintiffs’ allegation “that some indeterminate part of their premiums went toward paying for security measures” was “flimsy,” and the plaintiffs did “not maintain . . . that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime”).

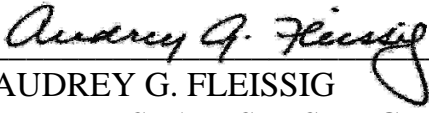
## **CONCLUSION**

Accordingly,

**IT IS HEREBY ORDERED** that Defendant's motion to dismiss the complaint with prejudice is **GRANTED**. ECF No. 24.

**IT IS FURTHER ORDERED** that all other pending motions are **DENIED** as moot.

A separate judgment shall accompany this Memorandum and Order.

  
\_\_\_\_\_  
AUDREY G. FLEISSIG  
UNITED STATES DISTRICT JUDGE

Dated this 13th day of November, 2017.